Pruvendo

Web 3 security company

- Development of secure smart contracts: Ethereum, MultiversX, Everscale, TON
- Formal verification of smart contracts
- Audit of smart contract and security checks

The high quality and security of smart contracts are vital. To **dramatically decrease the risk of hacks, attacks and unintended smart contract behaviour**, formal verification can be extremely useful - it allows to **prove that smart contract is correct against the formulated specification**, based on math theorem proving approach. However there are some serious obstacles prevent it from mass adoption:

- Extremely high cost - due to high demand to qualification of mathematicians performing it
- Extremely long duration - traditionally every property proved manually in proof assistant
- Absolute non-transparency for the customer

Pruvendo team developed the technology that is:

- **Fast** and cheap - now verification process can be finished in weeks
- **Semi-automated** - many properties can be proved automatically, also quick verification (randomised) is possible
- Allows the customer to **understand the approach and follow the process** till the very deep stage

The technology was probed at the Ethereum, MultiversX, Everscale blockchains where it proved to be useful and affordable, being **applied to secure the most critically important smart contracts.** Such, the rather big Multisig contract whose verification required **~30 man/months a few years ago, now took just 1** man/month, allowing to **find five critical bugs missed by all the audits**.

Pruvendo

CEO - Sergey Egorov

CTO - Andrey Lyashin

We strongly recommend to apply formal verification in conjunction with audit. It is crucial for smart contracts, exploits in which can lead to money and repetitional losses, especially with non-trivial logic.

team@pruvendo.com

pruvendo.com